KONINKRIJK DER NEDERLANDEN

Bureau voor de Industriële Eigendom

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

Hierbij wordt verklaard, dat in Nederland op 19 augustus 2002 onder nummer 1021300,

ten name van:

NEDERLANDSE ORGANISATIE VOOR TOEGEPAST-

NATUURWETENSCHAPPELIJK ONDERZOEK TNO

te Delft

een aanvrage om octrooi werd ingediend voor:

"Beveiliging van computernetwerk",

en dat de hieraan gehechte stukken overeenstemmen met de oorspronkelijk ingediende stukken.

Rijswijk, 29 augustus 2003

De Directeur van het Bureau voor de Industriële Eigendom,
voor deze,

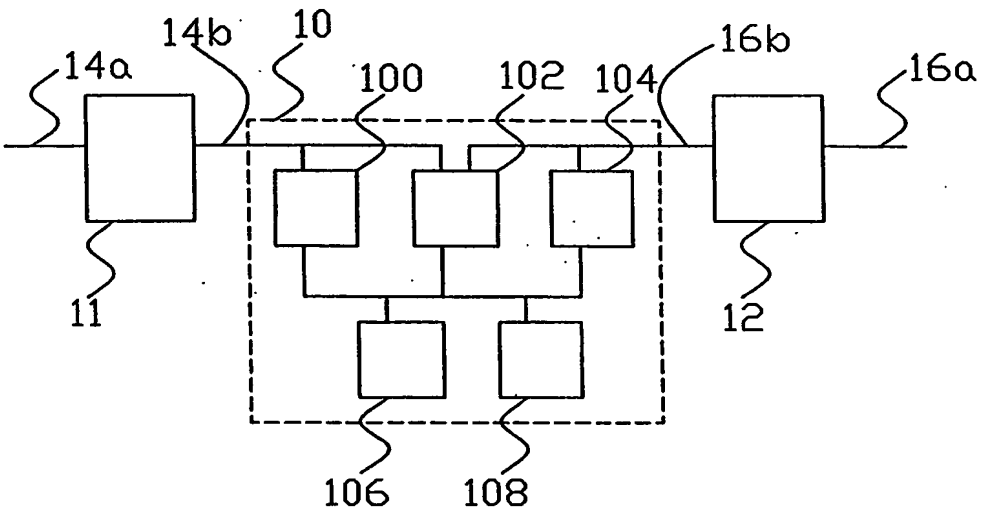
Mw. I.W. Scheevelenbos-de Reus

1021300

UITTREKSEL

Het computer systeem omvat een lokaal netwerkdomein van communicerende computers en een aansluiting voor communicatie met een extern netwerk. Een poortinrichting gekoppeld tussen het lokale netwerk en de aansluiting is ingericht om files die vanuit het lokale netwerk verzonden worden naar de aansluiting te controleren op aanwezigheid van een security-tag in het file, en om al dan niet doorzenden van elk file naar de aansluiting te besturen afhankelijk van detectie van de aan- of afwezigheid van de security-tag in het file.

7 11


14b
10
14a
100
102
104
16b
16a
11
12
106
108

1021300

P59620NL00

Titel: Beveiliging van computernetwerk.

De uitvinding heeft betrekking op beveiliging tegen ongeautoriseerde toegang (tot kopieën) van files die in een computer netwerk zijn opgeslagen.

Het is bekend in de huidige situatie dat om de vertrouwelijkheid van elektronische documenten (verder ook aangeduid als "files") te garanderen door in een filesysteem codes op te slaan die aan geven welke gebruikers het document mogen openen. Zo kan deze code bijvoorbeeld aangeven of alleen de auteur van het file, een toegangsrecht heeft of ook een groep waartoe deze auteur behoort, of dat eenieder een toegangsrecht heeft. Als een gebruiker een dergelijk file probeert te lezen dan controleert het beheerssysteem of de betreffende gebruiker volgens de codes voor het gevraagde file een toegangsrecht heeft. Alleen als dat het geval is staat het beheerssysteem toegang toe.

Deze vorm van toegangsbeheer heeft het nadeel dat ze gebonden is aan het filesysteem. Deze vorm van toegangsbeheer vereist dat gebruikers vooraf in verschillende soorten worden ingedeeld.

Een andere vorm van toegangsbeheer is het versleutelen (Engels: encrypten) van vertrouwelijke files. Alleen diegenen die beschikken over de sleutel die benodigd is voor het ontsleutelen van het file kunnen zodoende toegang krijgen. Het voordeel ten opzichte van toegangscodes is dat nu ook alle inhoudelijke kopieën van het file beschermd zijn, waar ze ook staan. Nadeel is echter dat telkens een sleutel en ontsleuteling nodig zijn voordat toegang tot het file mogelijk is.

Ter bescherming tegen computer virussen is het daarnaast bekend om gebruik te maken van een zogenaamde firewall voor het transport van files naar een computersysteem toe. Een firewall blokkeert het ontvangen van files door een computersysteem wanneer het file aan vooraf bepaalde karakteristieken voldoet. Een firewall dient echter niet voor het

vertrouwelijk houden van geselecteerde vertrouwelijke files tussen files die door het computersysteem verzonden worden.

Het is onder meer een doel van de uitvinding om te voorzien in een computer systeem dat het mogelijk maakt om de toegang tot files selectief te beperken zonder dat extra maatregelen nodig zijn als er kopieën gemaakt worden binnen het computersysteem en zonder dat versleuteling nodig is.

Het computersysteem volgens de uitvinding wordt gedefinieerd in conclusie 1. De uitvinding maakt gebruik van een poortinrichting in een communicatiekanaal tussen een netwerkdomein en een externe verbinding zoals een verbinding naar het Internet. De poortinrichting is ingericht om alle files die via het communicatiekanaal naar de externe verbinding verstuurd worden te controleren op de aanwezigheid van een security-tag . Afhankelijk van de aan- of afwezigheid van deze security-tag beperkt de poortinrichting de vrije verzending van het file naar de externe verbinding.

Zodoende wordt een file-selectieve controle uitgeoefend op de toegangsmogelijkheden tot het file buiten het netwerkdomein. Binnen het netwerkdomein heeft iedere gebruiker in principe toegang tot het file. Maar daarbuiten is de toegang beperkt. Zodoende wordt voorzien in een domeinspecifieke beveiliging. In de meest extreme vorm blokkeert de poortinrichting de verzending afhankelijk van de aan- of afwezigheid van deze security-tag . In principe kan de uitvinding op allerlei vormen van file verzending worden toegepast, bijvoorbeeld bij verzending als onderdeel van e-mail protocollen (SMTP), als onderdeel van file transfer protocollen (FTP) als onderdeel van hyperlink protocollen (HTTP) of elke andere soort protocol.

Bijvoorkeur worden alle communicatiekanalen van het netwerkdomein naar externe verbindingen voorzien van een dergelijke poortinrichting. In een uitvoeringsvorm beperkt de poortinrichting vrije verzending van files die voorzien zijn van een dergelijke security-tag .

Zodoende blijven bestaande of van extern ontvangen files vrij toegankelijk en kunnen gebruikers zelf bescherming vragen.

De uitvinding is echter niet beperkt tot volledig tegenhouden. In een andere uitvoeringsvorm versleutelt de poortinrichting bijvoorbeeld automatisch alle files die van een security-tag zijn voorzien als deze files via het communicatiekanaal verzonden worden. Zodoende wordt buiten het netwerkdomein bescherming geboden door middel van encryptie. In weer een ander uitvoeringsvorm wordt de security-tag gecombineerd met een anti-tamper code die het verwijderen van tag de vrijwel onmogelijk maakt.

Deze en andere doelstellingen en voordelige aspecten van het computersysteem volgens de uitvinding zullen nader worden beschreven aan de hand van de volgende figuren.

Figuur 1 toont een computer systeem
Figuur 2 toont een poortinrichting

Figuur 1 toont een computer systeem met externe aansluitingen 14a, 16a. Het computersysteem bevat een domein 10 met daarin een aantal computers 100, 102, 104, 106, 108 die via verbindingen met elkaar verbonden zijn. Een deel van de computers 100, 102, 104, 106, 108 is verbonden met communicatiekanalen 14a,b, 16a,b die via de externe aansluitingen lopen naar verdere computers (niet getoond). In de communicatiekanalen 14a,b, 16a,b bevinden zich poortinrichtingen 11, 12. De poortinrichtingen maken elk bijvoorkeur deel uit van een inrichting die ook andere veiligheidstaken heeft, zoals het effectueren van een firewall e.d. In gebruik worden in één of meer van de computers in domein 10 files opgeslagen. Die via de verbindingen vanuit alle computers in het domein gelezen kunnen worden. Deze files kunnen voorzien worden van "security-tags". In een HTML file zou de security-tag bijvoorbeeld kunnen worden

geïmplementeerd door toevoeging van een stuk tekst in de vorm van <SECURITY> </SECURITY>, eventueel aangevuld met parameters. Uiteraard kan de security-tag op allerlei andere wijzen uitgevoerd worden, bijvoorbeeld door toevoeging van andere soorten codes, of door het aanbrengen van een watermerk in het file. Bijvoorkeur is de computer ingericht om het file of het belangrijkste deel daarvan bij het aanbrengen van het security-tag ook automatisch te encrypten. Zodoende wordt een extra beveiliging gerealiseerd.

Wanneer een file vanuit een computer in het domein via één van de communicatiekanalen naar één van de externe aansluitingen 14a, 16a verstuurd wordt gebeurt dit via poortinrichting 11 of 12. De desbetreffende poortinrichting 11, 12 controleert het file op de aanwezigheid van de security-tag alvorens het file door te sturen naar de externe aansluiting 14a, 16a. Poortinrichting 11, 12 stuurt het file alleen door als het de security-tag niet aantreft. Bijvoorkeur slaat poortinrichting 11, 12 daarnaast gegevens over de verzending van het file op in een log file, tenminste als de verzending is tegengehouden. Dit stelt de systeembeheerder in staat later op overtredingen te controleren.

Figuur 2 toont een uitvoeringsvorm van een poortinrichting 11 in meer detail. De poortinrichting 11 bevat een eerste transceiver 20 voor het lokale deel van het communicatiekanaal 14b, een tweede transceiver 22 voor de externe aansluiting 14a, een geheugen 24 en een tag detector 26. Transceivers 20, 22 zijn aan geheugen 24 gekoppeld. Detector 26 heeft een ingang gekoppeld aan eerste transceiver 20 voor het lokale deel van het communicatiekanaal 14b en een uitgang gekoppeld aan tweede transceiver 22 voor de externe aansluiting 14a.

In bedrijf ontvangt eerste transceiver 20 boodschappen van het lokale deel van het communicatiekanaal 14b en slaat deze boodschappen tijdelijk op in geheugen 24. Detector 26 onderzoekt de inhoud van de boodschap op aanwezigheid van een file met daarin een security-tag en stuurt, afhankelijk

van een resultaat van dat onderzoek, een commando naar tweede transceiver 22. Wanneer het commando ertoe strekt om de boodschap door te laten leest tweede transceiver 22 de boodschap uit geheugen 24 en verstuurt de boodschap naar externe aansluiting 14a. Wanneer de boodschap niet doorgestuurd wordt, wordt de boodschap uit geheugen 24 verwijderd bijvoorbeeld door deze met een latere boodschap te overschrijden zonder dat de boodschap is doorgestuurd.

De computers in domein 10 zijn ingericht om de betrokken files zonder controle op de security-tag op alle computers in domein te lezen of te kopiëren. Zodoende is het mogelijk in domein 10 op willekeurige plaatsen files op te slaan en te kopiëren, maar wordt ongewenst of per ongeluk versturen naar externe aansluitingen 14a,b buiten het domein onmogelijk gemaakt.

Zonder van het principe van de uitvinding af te wijken zijn uiteraard allerlei andere uitvoeringsvormen mogelijk. Zo kan poortinrichting 11, 12 bijvoorbeeld het file juist niet doorsturen als géén security-tag aanwezig is. Daardoor kan een gebruiker er bewust voor kiezen een file tegen versturen te beschermen.

Als onderdeel van de beveiliging kan een tamper beveiliging opgenomen worden, zoals bijvoorbeeld een met een private key versleutelde code, die met een public key ontsleuteld kan worden en die een getal bevat dat een functie is van de inhoud van het file inclusief security-tag. Alvorens het file te verzenden kan de poortinrichting dan de code opnieuw berekenen aan de hand van het file en vergelijken met de code die door public key ontsleuteling uit het file volgt. Zodoende wordt voorkomen dat de security-tag kan worden gewijzigd. Ook kan het tag als een watermerk in bepaalde soorten files worden opgenomen.

Verder kan poortinrichting 11, 12, in plaats van het file niet te versturen, het file versleutelen alvorens het te versturen, wanneer de security-tag aangeeft dat vrij versturen niet is toegestaan. Desgewenst kan zelfs met

parameters in het security-tag worden aangegeven welke behandeling (bijvoorbeeld niet versturen of versleuteld versturen) het file bij het passeren van poortinrichting 11, 12 moet ondergaan.

CONCLUSIES

1. Een computer systeem, voorzien van
- een lokaal netwerkdomein van communicerende computers;
- een aansluiting voor communicatie met een extern netwerk;
- een poortinrichting gekoppeld tussen het lokale netwerk en de aansluiting, welke poortinrichting is ingericht om files die vanuit het lokale netwerk verzonden worden naar de aansluiting erop te controleren dat zij een security-tag bevatten, en om al dan niet doorzenden van elk file naar de aansluiting te besturen afhankelijk van detectie van de aan- of afwezigheid van de security-tag in het file.

2. Een computer systeem volgens conclusie 1, waarin de poortinrichting is ingericht om doorzenden van het file te blokkeren als de security-tag in het file aanwezig is.

3. Een computer systeem volgens conclusie 1 of 2, waarin de communicerende computers zijn ingericht om bij het aanbrengen van de security-tag een substantieel deel van het file te encrypten.

4. Een poortinrichting met een koppeling voor aansluiting van een lokaal netwerk en een aansluiting voor een extern netwerk, welke poortininrichting is ingericht om files die vanuit het lokale netwerk verzonden worden naar de aansluiting erop te controleren of zij een security-tag bevatten, en om al dan niet doorzenden van elk file naar de aansluiting te besturen afhankelijk van detectie van de aan- of afwezigheid van de security-tag in het file.

5. Een werkwijze voor het beveiligen van informatietransport van een lokaal netwerk naar een extern netwerk, welke werkwijze de stappen omvat van
- aanbrengen van een security-tag in geselecteerde files;

- onderzoeken van files die door een poortinrichting van het lokale netwerk naar het externe netwerk verzonden worden op aanwezigheid van de security-tags;
- het blokkeren of doorzenden van die files waarin een security-tag aanwezig is.

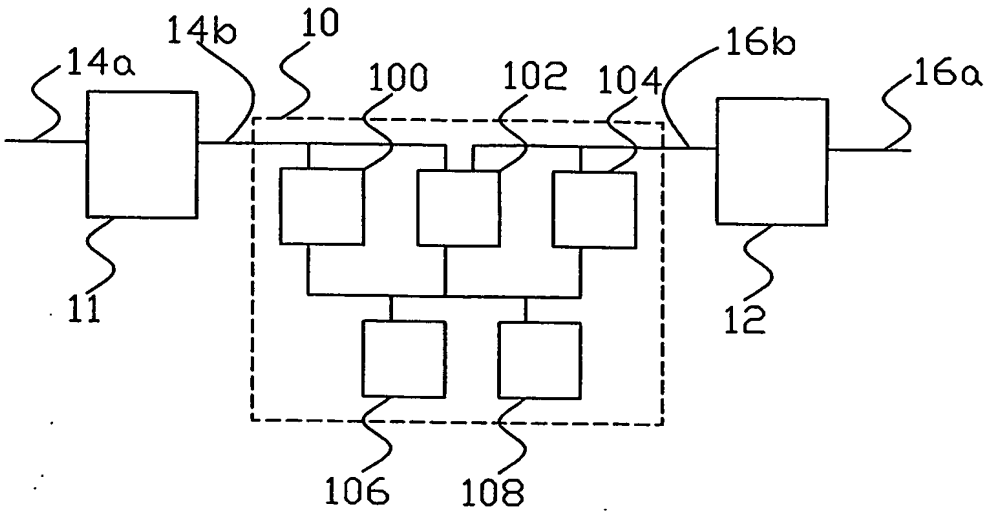


Fig. 1

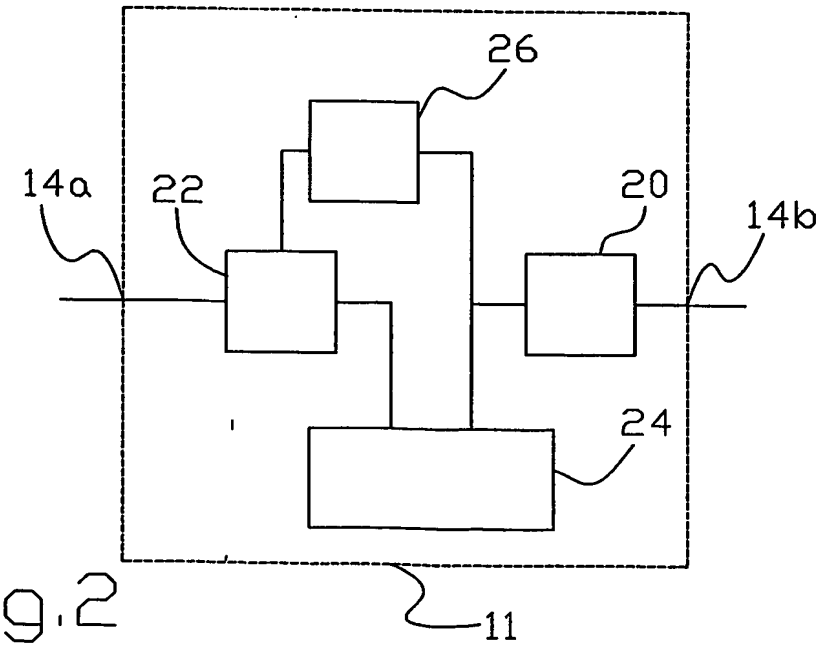


Fig. 2